THE USE OF RENEWABLE AND DISTRIBUTED TECHNOLOGIES TO IMPROVE ENERGY SECURITY ON MILITARY FACILITIES

Renewable Working Group Meeting
Washington, DC
April 2, 2002

Abbas Akhil, Energy Security Department
(aaakhil@sandia.gov)
and
Dave Menicucci, Defense Energy Support Program
(dfmenic@sandia.gov)

Sandia National Laboratories
Albuquerque, NM

Presentation Outline

1. Overview of Sandia National Labs
2. Review of security-related issues of this work
3. Basic concepts and generic examples
4. Role of distributed and renewable technologies
5. Summary

Some Background on Sandia Laboratories

- Largest DOE National Lab, 8000 staff; $1.4B
- Multi-program, systems engineering lab with defense emphasis
- Work in renewable energy for 25 years—longer than any other lab

- Several test labs in renewable and distributed energy resources
- Security issues are among Sandia's core competencies
  - Sandia/LANL recently funded to develop the National Infrastructure Simulation and Analysis Center
  - Sandia is currently working with two bases on security and renewables project

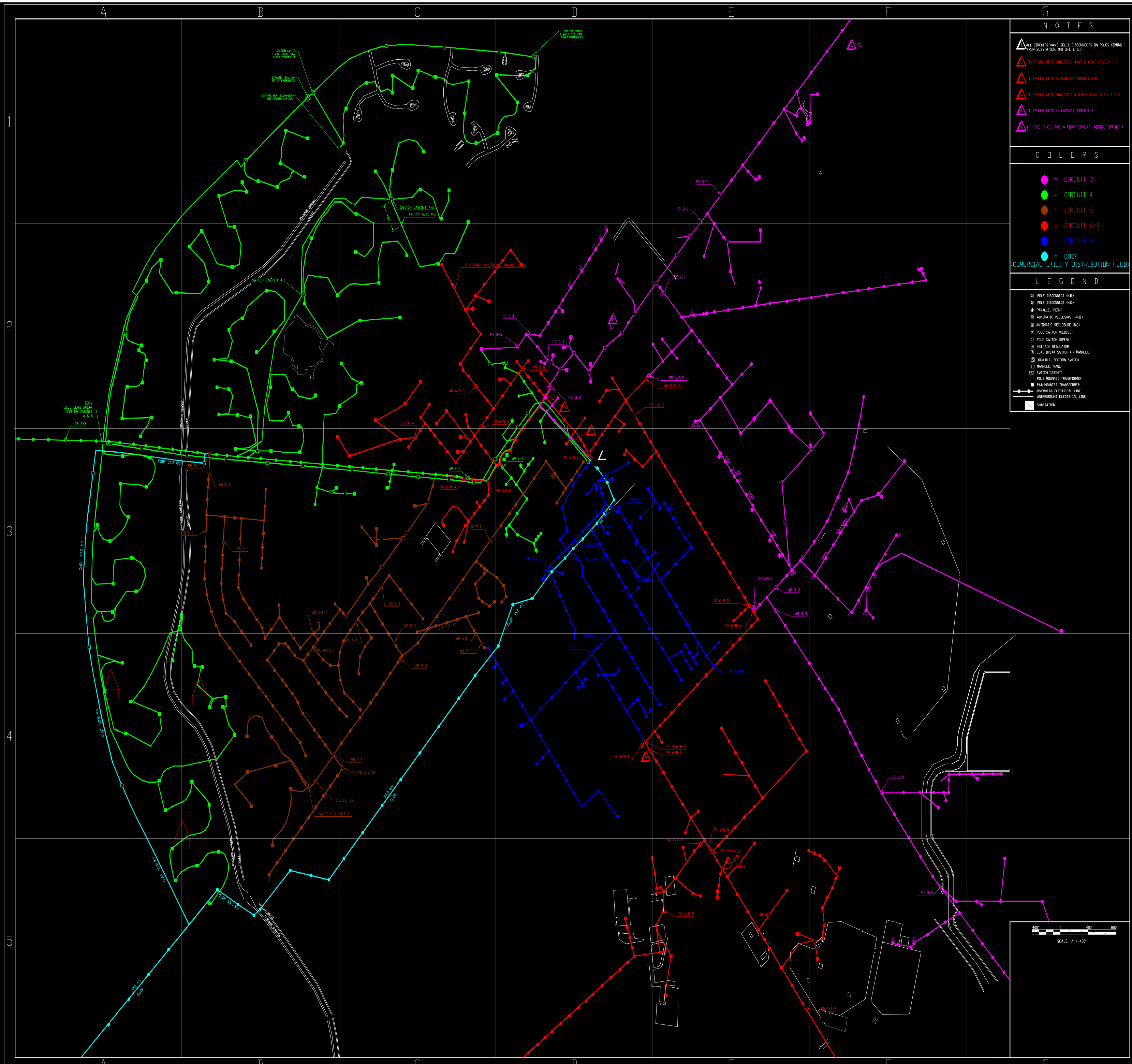
Energy Security Analysis Has Strategic Value

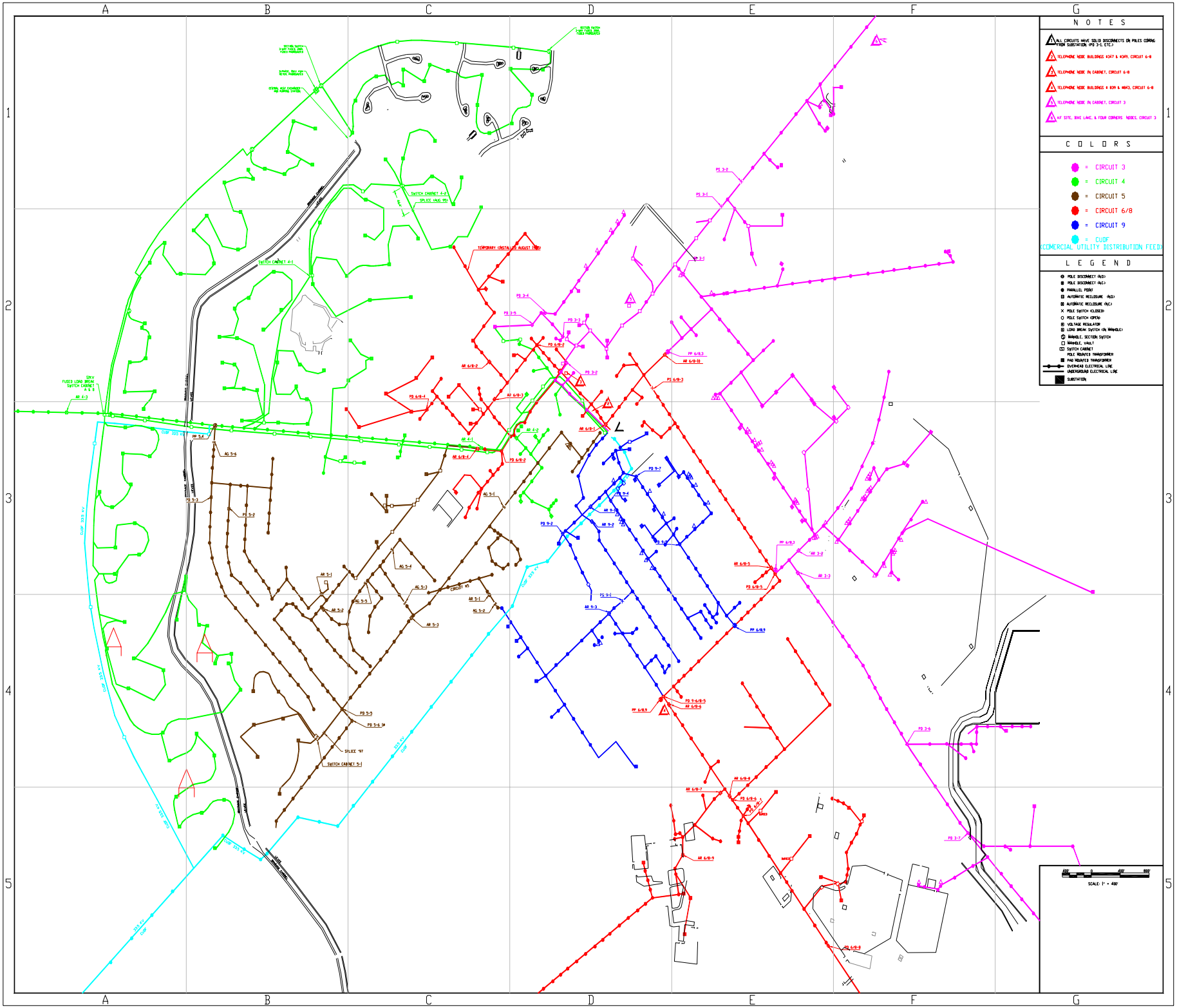
- Energy systems are critical infrastructure components of military bases
  - Electricity and gas; inter-dependencies with water; command and control
  - Energy infrastructures presently offer easy targets – from simply annoying to severely impacting mission critical activities
  - Must be given high priority for protection
- Security analysis reveals vulnerabilities that could be exploited by terrorists
  - Analysis must be conducted in an appropriately secure facility by cleared personnel
    - Sandia conducts its work in a Top Secret (Q) or Secret (L) environment

No classified information presented in this talk

Only generic information is discussed with no details

More information can be provided to cleared individuals with a need-to-know


N O T E S
1 ALL CIRCUITS HAVE SOLID DISCONNECTS ON POLES COMING FROM SUBSTATION. (PD 3-1, ETC.)
2 TELEPHONE NODE BUILDINGS #347 & #349, CIRCUIT 6-8
3 TELEPHONE NODE IN CABINET, CIRCUIT 6-8
4 TELEPHONE NODE BUILDINGS # 839 & #843, CIRCUIT 6-8
5 TELEPHONE NODE IN CABINET, CIRCUIT 3
6 H.F SITE, BIKE LAKE, & FOUR CORNERS NODES, CIRCUIT 3
C O L O R S
= CIRCUIT 3
= CIRCUIT 4
= CIRCUIT 5
= CIRCUIT 6/8
= CIRCUIT 9
= CUDF
(COMERCIAL UTILITY DISTRIBUTION FEED)
L E G E N D
POLE DISCONNECT (N.O.)
POLE DISCONNECT (N.C.)
PARALLEL POINT
AUTOMATIC RECLOSURE (N.O.)
AUTOMATIC RECLOSURE (N.C.)
POLE SWITCH (CLOSED)
POLE SWITCH (OPEN)
VOLTAGE REGULATOR
LOAD BREAK SWITCH (IN MANHOLE)
MANHOLE, SECTION SWITCH
MANHOLE, VAULT
SWITCH CABINET
POLE MOUNTED TRANSFORMER
PAD MOUNTED TRANSFORMER
OVERHEAD ELECTRICAL LINE
UNDERGROUND ELECTRICAL LINE
SUBSTATION
SWITCH CABINET 4-2
SWITCH CABINET 4-1
SWITCH CABINET 5-2
CUDF 33.5 KV


NOTES
ALL CIRCUITS HAVE SOLID DISCONNECTS ON POLES COMING FROM SUBSTATION, (PD 3-1, ETC.)
TELEPHONE NODE BUILDINGS #347 & #349, CIRCUIT 6-8
TELEPHONE NODE IN CABINET, CIRCUIT 6-8
TELEPHONE NODE BUILDINGS # 829 & #843, CIRCUIT 6-8
TELEPHONE NODE IN CABINET, CIRCUIT 3
H.F. SITE, BIKE LANE, & FOUR CORNERS NODES, CIRCUIT 3
COLORS
= CIRCUIT 3
= CIRCUIT 4
= CIRCUIT 5
= CIRCUIT 6/8
= CIRCUIT 9
= CUDF
COMERCIAL UTILITY DISTRIBUTION FEED
LEGEND
POLE DISCONNECT (NO)
POLE DISCONNECT (NC)
PARALLEL POINT
AUTOMATIC RECLOSURE (NO)
AUTOMATIC RECLOSURE (NC)
POLE SWITCH CLOSED
POLE SWITCH OPEN
VOLTAGE REGULATOR
LOAD BREAK SWITCH (IN MANHOLE)
MANHOLE, SECTION SWITCH
MANHOLE, VAULT
SWITCH CABINET
POLE MOUNTED TRANSFORMER
PAD MOUNTED TRANSFORMER
OVERHEAD ELECTRICAL LINE
UNDERGROUND ELECTRICAL LINE
SUBSTATION
SCALE: 1" = 400'
A
B
C
D
E
F
G
1
2
3
4
5

Vulnerability of Off-base Electric Infrastructure

- Off-base facilities and information owned by electric utilities
  - Substations, switchyards, poles, cables
  - One-line diagrams, maps, access and control of key facilities
  - **Controlling this access and information off-base may not be practical or enforceable**
- Sample vulnerabilities
  - Single feeder to base – poles and conductor easily taken out with low probability of detection
    - Line restoration could exceed several days
  - Substation transformers and hardware – disabled with readily available tools such as a rifle or a hand drill
    - Transformers, breakers and other hardware are long-lead time items – spares are not usually stocked by the utility
    - Outage could last several months depending on spares availability

Vulnerability of On-base Electric Infrastructure

- Unlike off-base facilities, controlling information and access to on-base facilities is achievable
- On-base electric infrastructure elements are basically similar
  - Substations, switchyards, poles, cables
  - Except on-site and stand-by generators, physical plant and special use facilities and fuel storage bunkers
- Protection needed includes controlling physical access, camouflaging thermal and noise signatures
- Typical vulnerabilities
  - Sabotaging substation, stand-by generation and UPS equipment
  - Coordinated outages programmed through building energy management systems

Terrorist Attack Strategy

- Use low-tech tools and low profile approach

- Cut the utility feeder line to base
  - Approach: Spot key structural poles and shoot conductor and insulators
  - Tools: .30-06 rifle with scope, ordinary ammo; one horse or ATV optional
  - Damage: Possible base-wide outage of 1 – 3 days while line is rebuilt

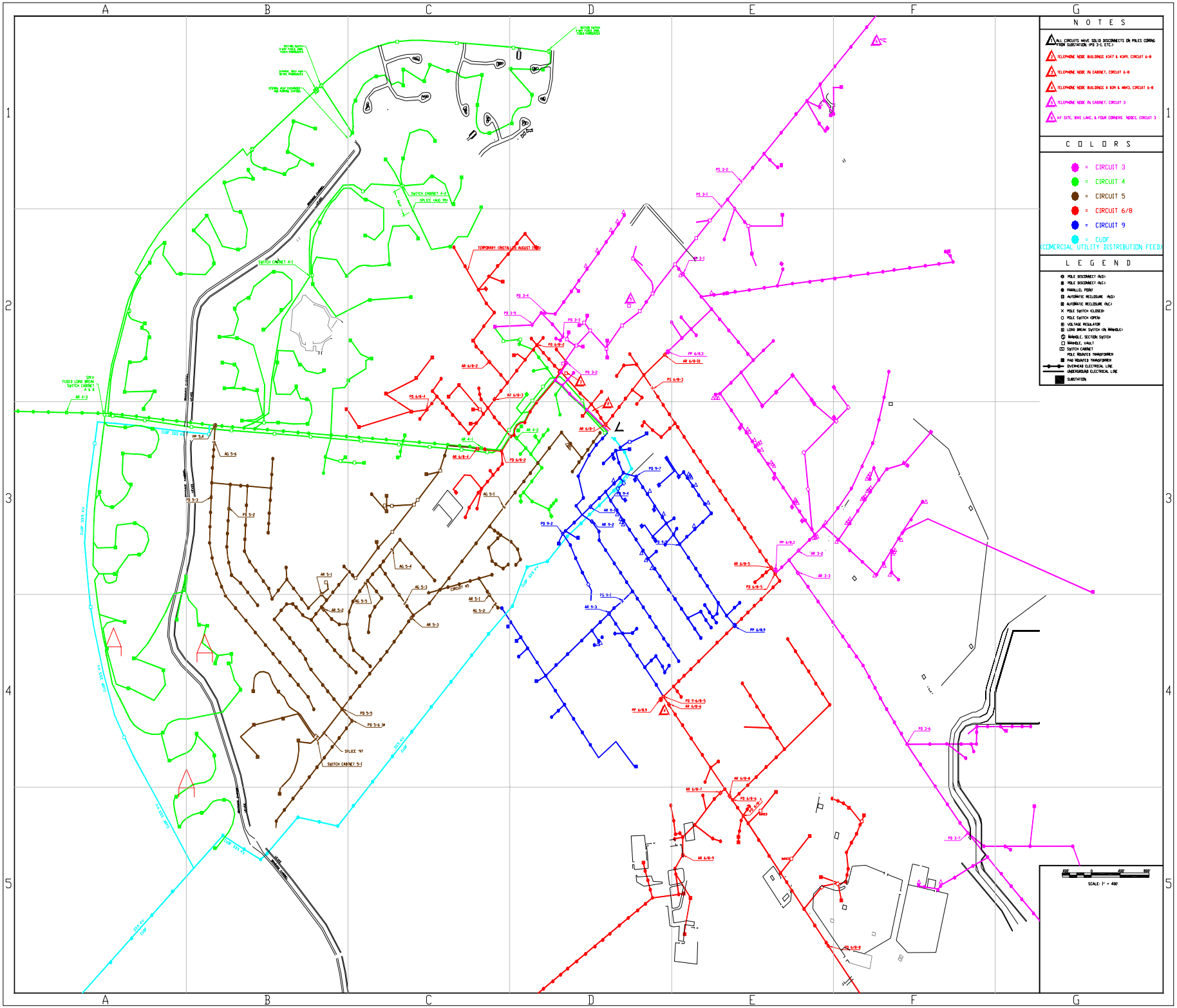
- Disable key substation transformer(s) – On or Off-base
  - Approach: Break into substation and loosen transformer oil drain plug
  - Tools: Padlock cutter, hex wrench
  - Damage: Burnt transformers; replacement takes 3 – 6 months based on transformer size and availability; base power supply curtailed or severely limited for extended time period.

Role of Distributed and Renewable Sources

- Distributed resources are inherently dispersed and represent incrementally small power blocks
  - Less threat exposure than centralized generation
  - Distributed resources can be mobile
  - Size ranges from 10 kW to 3 MW
  - Mobility decreases threat risk
    - Generator location changes unexpectedly and frequently

Different Integration Approach

- Pre-plan and build supporting infrastructure to respond in event of attack
- Identify and prepare several “nodes” where (mobile) distributed generation could be tied in quickly
  - Sectionalize distribution as necessary to isolate and serve critical loads/facilities
  - Fuel source availability – supply or storage
  - Move switchgear underground or tightly integrate in building design
  - Reduce thermal and noise signatures


NOTES
ALL CIRCUITS HAVE SOLID DISCONNECTS ON POLES COMING FROM SUBSTATION, (PD 3-1, ETC.)
TELEPHONE NODE BUILDINGS #347 & #349, CIRCUIT 6-8
TELEPHONE NODE IN CABINET, CIRCUIT 6-8
TELEPHONE NODE BUILDINGS # 829 & #843, CIRCUIT 6-8
TELEPHONE NODE IN CABINET, CIRCUIT 3
H.F. SITE, BIKE LANE, & FOUR CORNERS NODES, CIRCUIT 3
COLORS
= CIRCUIT 3
= CIRCUIT 4
= CIRCUIT 5
= CIRCUIT 6/8
= CIRCUIT 9
= CUDF
COMERCIAL UTILITY DISTRIBUTION FEED
LEGEND
POLE DISCONNECT (NO)
POLE DISCONNECT (NC)
PARALLEL POINT
AUTOMATIC RECLOSURE (NO)
AUTOMATIC RECLOSURE (NC)
POLE SWITCH CLOSED
POLE SWITCH OPEN
VOLTAGE REGULATOR
LOAD BREAK SWITCH (IN MANHOLE)
MANHOLE, SECTION SWITCH
MANHOLE, VAULT
SWITCH CABINET
POLE MOUNTED TRANSFORMER
PAD MOUNTED TRANSFORMER
OVERHEAD ELECTRICAL LINE
UNDERGROUND ELECTRICAL LINE
SUBSTATION
SCALE: 1" = 400'
A
B
C
D
E
F
G
1
2
3
4
5

Summary

- Energy security analysis must be performed in an appropriate controlled environment
- Military bases are increasingly conscious of energy infrastructure vulnerabilities. RE and DER could be a key element of the solutions portfolio
- Off-base and on-base electric infrastructures share similarities but vulnerabilities differ
- RE and DER can play a key role in enhancing survivability and operational continuity under severe threat conditions